


CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service in an envelope as "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 C.F.R.1.10, Mailing Label No. EV697450103US and is addressed to the: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Date: May 1, 2006


Wilburn Liddell, Jr.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Dorothy Denning et al.

Serial No.: 09/992,378

Filed: November 16, 2001

Title: SYSTEM AND METHOD FOR
DELIVERING ENCRYPTED INFORMATION
IN A COMMUNICATION NETWORK USING
LOCATION IDENTITY AND KEY TABLES

Art Unit: 2134

Examiner: Piotr Poltorak

Attorney Docket No.: 774070-8

05/04/2006 SHASSEN1 00000104 09992378

02 FC:2402

250.00 0P

APPEAL BRIEF

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellant filed a Notice of Appeal in the above-identified application on February 7, 2006 under 35 U.S.C. § 134(a), and hereby submits this Appeal Brief under 37 C.F.R. § 41.37 concurrently with a Petition for Extension of Time pursuant to 37 C.F.R. § 1.136. Appellant respectfully submits that this Appeal Brief is timely filed under 37

C.F.R. § 41.37(a)(1), and the Appeal Brief meets the substantive requirements of § 41.37(c)(1). Appellant requests entry, consideration, and favorable action on this appeal at the Board's earliest convenience.

In accordance with § 41.37(c)(1), Appellant presents the following items under the headings prescribed therein.

Real Party in Interest

GeoCodex LLC is the real party in interest as assignee of the subject application pursuant to an assignment recorded at reel 014140, frame 0199.

Related Appeals and Interferences

Neither the assignee nor Appellant is aware of any other appeals or interferences that would bear on the Board's decision in this appeal.

Status of Claims

Claims 1-6, 8-32, and 34-50 stand finally rejected in the Office Action dated September 7, 2005, and are under appeal pursuant hereto. Claims 7 and 33 were previously cancelled.

Status of Amendments

Appellant submitted proposed amendments to Claims 5, 6, 14, 15, and 46 on February 27, 2006. An Advisory Action dated March 29, 2006 indicates that the proposed amendments are entered for purposes of appeal.

Summary of Claimed Subject Matter

The invention pertains generally to the secure communication of encryption keys between a sender and a receiver. In the field of cryptography, it is known to use a key (e.g., an alphanumeric code sequence) to encrypt a data file. To support subsequent secure communications between a sender and a receiver, the key must be passed from the sender to the receiver. To avoid the risk of interception of the key by an unauthorized receiver, the invention provides a novel method of communicating the key in encrypted form from the sender to the receiver. More particularly, the invention contemplates the encryption of the key using information that defines a specific location. The encrypted key may then be passed to a receiver. The receiver will be able to decrypt the encrypted key only if the receiver is located at the unique location that had been used originally to encrypt the key. Hence, if the receiver is not located at the unique location (i.e., an unauthorized receiver), the receiver cannot decrypt the key, and therefore cannot decrypt the data message.

As illustrated in Fig. 5 (below), plaintext data is encrypted using a random data encrypting key that is generated at the time of encryption (see step 516 and page 19, lines 21-22). The data encrypting key is then encrypted (or locked) using a location value and a key encrypting key (see step 522 and page 19, lines 22-25). This is a two-step process that involves (1) using the location value to modify the data encrypting key to produce a location-modified data encrypting key, and (2) encrypting the location-modified data encrypting key using the key encrypting key (see page 26, line 24 through page 27, line 1). The encrypted location-modified data encrypting key and the ciphertext data is then transmitted to the receiver (see page 19, lines 25-27). These aspects of the invention are defined in Claims 1-6, 8-15 and 18-20 that recite a method for controlling access to digital information, and in Claims 28-32, 34-37 and 39-40 that recite an apparatus for controlling access to digital information.

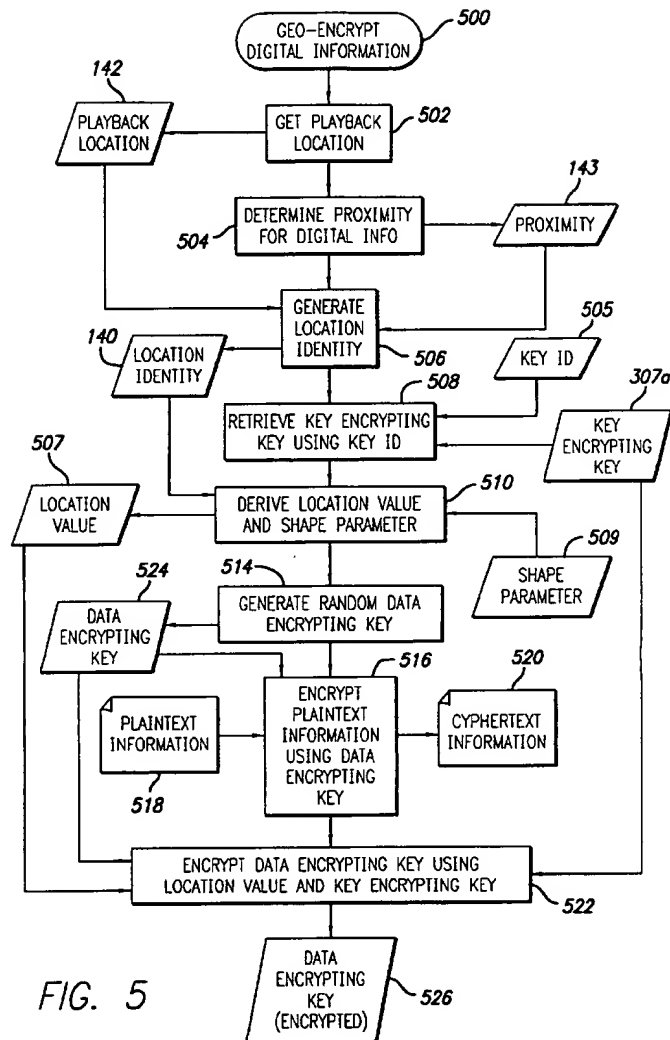


FIG. 5

The receiver must be at the correct location and must have a copy of a corresponding key decrypting key in order to decrypt the encrypted location-modified data encrypting key and extract the data encrypting key from the location-modified data encrypting key. As illustrated in Fig. 6 (below), the receiver will decrypt the location-modified data encrypting key using the key decrypting key and a location value derived from the known location of the receiver (see step 612 and page 20, lines 26-27). This is a two-step process that involves (1) using the key decrypting key to decrypt the location-modified data encrypting key, and (2) using the location value to recover the

data encrypting key (see page 28, lines 5-11). Thereafter, the receiver will decrypt the encrypted digital information using the decrypted data encrypting key (see step 614 and page 21, lines 1-2). These aspects of the invention are defined in Claims 45-48 that recite an apparatus for receiving digital information.

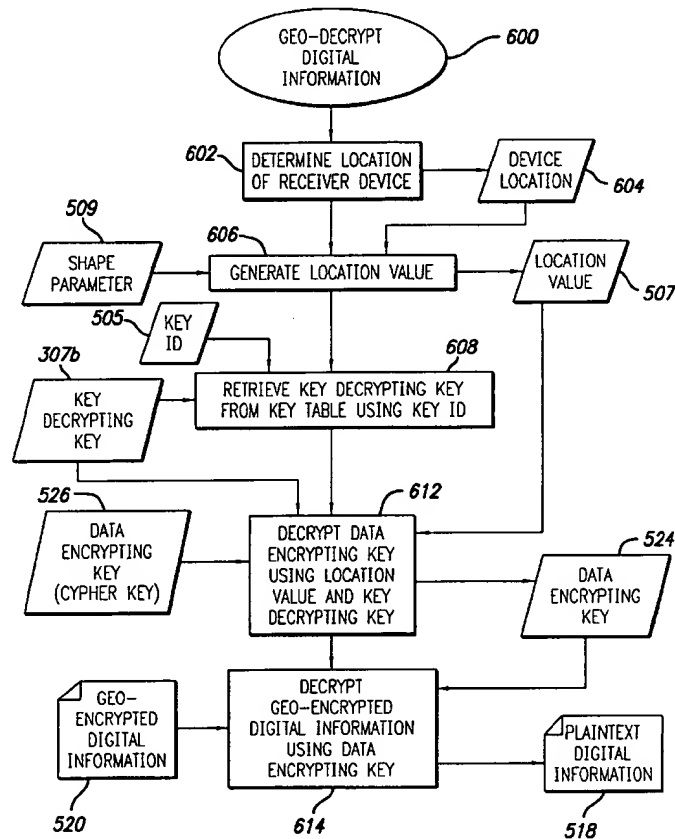


FIG. 6

Another embodiment of the invention provides a method and system for managing the various keys used by the sender and receiver to encrypt/decrypt digital information and/or keys. A key table associated with the sender or receiver may include plural keys. Each key may be used with a particular type of digital information. For example, in the context of the communication of digital television signals, the keys may be owned by particular content providers (e.g., HBO, Disney, ESPN, etc.) (see page 31,

lines 22-26). The invention provides certain management functions that enable the key owner to remotely add, change or delete keys from the user's key table (see page 31, lines 26-30), without the knowledge or intervention of the user. These aspects of the invention are defined in Claims 21-27, 41-44 and 49-50.

In yet another embodiment of the invention, the encrypted digital information can be routed through one or more intermediary distributors before being transmitted to a final receiver. One method for routing the encrypted digital information through a distributor involves encrypting the data encrypting key first with a location value and a key encrypting key for the final receiver and then with a location value and a key encrypting key for the distributor. The distributor removes its layer of encryption from the key before forwarding it to the receiver (see page 28, line 26 through page 29, line 1). With this method, none of the distributors can decrypt the data encrypting key because it remains encrypted with the location value and key encrypting key for the final receiver. These aspects of the invention are defined in Claims 16-17 and 38.

Each of the foregoing aspects of the invention are advantageous in ensuring the secure communication of digital information. As further discussed below, these embodiments are not suggested or disclosed by the prior art.

Grouping of Claims

Appellant groups the rejected claims as follows:

Group I: Claims 1-6, 8-15, 18-20, 28-32, 34-37 and 39-40

Group II: Claims 45-48;

Group III: Claims 21-27, 41-44 and 49-50; and

Group IV: Claims 16-17 and 38.

The claims within each of the above groups stand or fall together with respect to the pending rejections. In the arguments below, Appellant presents reasons why each group of claims is separately patentable over the cited references.

Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejection are reviewed in this appeal:

(a) Claims 1, 8, 11, 13-16, 28, 34, 37-38, and 45-46 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes ("Handbook of Applied Cryptography") in view of Laurence et al. (U.S. Patent No. 4,860,352);

(b) Claims 2-6, 9-10, 12, 18-19, 29-31, 35-36, 39, and 47 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Murphy (U.S. Patent No. 6,317,500);

(c) Claims 21-27, 41-44, and 49-50 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Schneier ("Applied Cryptography, Protocol, Algorithms and Source Code in C");

(d) Claim 19 stands finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and Schneier and further in view of Murphy;

(e) Claim 21-27 and 41-44 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Shibata et al. (U.S. Patent No. 5,586,185);

(f) Claim 17, 20, 40 and 48 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and Inoue et al. (U.S. Patent No. 6,240,514); and

(g) Claim 17, 20, 40 and 48 stand finally rejected under 35 U.S.C. § 103(a) as unpatentable over Menezes in view of Laurence et al. and further in view of Jones et al. (U.S. Patent No. 6,434,699).

Argument

I. Legal Standards

MPEP § 2143 states the basic requirements for a *prima facie* case of

obviousness under § 103(a) as follows:

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Furthermore, a prior art reference must be considered in its entirety, that is, as a whole, including portions that would lead away from the claimed invention. M.P.E.P. § 2141.02; *Bausch & Lomb v. Barnes-Hind/Hydrocurve, Inc.*, 796 F.2d 443, 448, 230 USPQ 416, 420 (Fed. Cir. 1986). As the Court in *Bausch & Lomb* affirmed, "[i]t is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one skilled in the art." *Id.*, citing *In re Wesslau*, 353 F.2d 238, 241, 147 USPQ 391, 393 (CCPA 1965). Among other things, it is improper to combine references without consideration for parts of the references that would have led one of ordinary skill away from the invention. *Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 281, 296-97, 227 USPQ 657, 669 (Fed. Cir. 1985); M.P.E.P. § 2145(X)D(2).

Indeed, a finding that a reference suggests the line of development flowing from its disclosure is unlikely to be productive of the result sought by the applicant can be sufficient to defeat a case of obviousness. *Winner Intern. Royalty Corp. v. Wang*, 202 F.3d 1340, 1350, 53 USPQ2d 1580, 1589 (Fed. Cir. 2000). Moreover, even if the cited references themselves do not expressly teach away from the invention, the prior art must be considered as a whole, as it would have been viewed by one of ordinary skill in the art. *In re Hedges*, 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed. Cir. 1986). For

example, proceeding contrary to accepted wisdom in the art is strong evidence of nonobviousness. *Id.*; M.P.E.P. § 2145(X)D(3).

In general, a rejection for obviousness based on a combination of references must be based on a "thorough and searching" factual inquiry using objective evidence of record. *In re Sang Su Lee*, 277 F.3d 1338, 1343, 61 USPQ2d 1430, 1434 (Fed. Cir. 2002). "This precedent has been reinforced in myriad decisions, and cannot be dispensed with." *Id.* "Evidence that supports, rather than negates, patentability must be fairly considered." *In re Dow Chemical Co.*, 837 F.2d 469, 473, 5 USPQ.2d 1529, 1533 (Fed. Cir. 1988). In the present application, the Examiner has performed no such factual inquiry of the evidence as a whole. Instead, the Examiner has improperly picked and chosen isolated portions of references to reconstruct the invention using hindsight, while ignoring substantial portions of the record that would support a conclusion of patentability.

II. The Rejections Fail To Establish A *Prima Facie* Case Of Obviousness For Any Of The Four Groups Of Claims

Appellant respectfully submits that the final Office Action fails to state a *prima facie* case of obviousness for at least two reasons. First, there is no suggestion or motivation in the references for the proposed combination. Second, even assuming the combination is proper, the proposed combination fails to teach or suggest all limitations of the claims. This Appeal Brief considers these issues for each of the four groups of claims.

A. Group I (Claims 1-6, 8-15, 18-20, 28-32, 34-37 and 39-40)

Independent Claim 1 of Group I is directed to a method for controlling access to digital information having the following four limitations:

encrypting said digital information using a data encrypting key;
modifying the data encrypting key using location identity data that

defines at least a specific geographic location to produce a location-modified data encrypting key;

encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key; and

communicating said encrypted location-modified data encrypting key and said encrypted digital information to a recipient device such that said encrypted digital information can be decrypted by the recipient only at said specific geographic location.

Independent Claim 28 of Group I is directed to an apparatus for controlling access to digital information. Hence, the claims of Group I are directed primarily to the encryption and communication of digital information and the data encrypting key in a manner in which the data encrypting key can only be recovered by a receiver located at a specific geographic location. In other words, the claims of Group I cover the sender side of the communication interface.

1. There is no suggestion or motivation in the references for the proposed combination of Menezes and Laurence et al.

Menezes provides a general text showing the current state of cryptography. The final Office Action asserts that Menezes' disclosure of "point-to-point key update using symmetric encryption" would read on "producing an encrypted location-modified data encrypting key produced by encrypting the data encrypting key using a key encrypting key." Appellant respectfully disagrees. Menezes discloses a key transport protocol in which a random number selected as the session key is encrypted using a known encryption algorithm and key (see p. 497). This encrypted session key is then communicated to the recipient. Once decrypted, the session key would then be used by the recipient to decrypt communications received from the originator.

Unlike the present invention, Menezes includes no teaching or suggestion of a "location-modified data encrypting key" or the desirability of modifying a data encrypting key using location information. The final Office Action plainly acknowledges this

deficiency, stating that “Menezes does not explicitly teach modifying the data encrypting key using location identity data that defines at least a specific geographic location.” As discussed above, the patent application enables a significant improvement in communication security over Menezes by providing that the recipient can decrypt the message only if (1) it has the appropriate key decrypting key, and (2) it is located at the specific geographic location defined by the location identity data.

To make up for the deficiency of Menezes, the final Office Action proposes the combination with Laurence et al. Appellant submits that there is no suggestion or motivation for the proposed combination of Menezes and Laurence et al., and that there is no *prima facie* showing of obviousness for at least this reason.

As a fundamental matter, the final Office Action improperly equates two protocols that are known within the field of encryption: key exchange and authentication. Key exchange refers to the process by which encryption keys are exchanged among users so that they may communicate using a common encryption algorithm. See, e.g., http://en.wikipedia.org/wiki/Key_exchange. The citation from Menezes describes a form of key exchange referred to as “point-to-point key update.” In contrast, authentication refers to the process of attempting to verify the identity of the sender of a communication. See, e.g., <http://en.wikipedia.org/wiki/Authentication>. As discussed below, authentication is the objective of Laurence et al. Key exchange and authentication are different protocols that serve different objectives, and it would not be obvious to use an authentication teaching to solve a key exchange problem.

More particularly, Laurence et al. is directed to a system for authenticating data transmissions in order to protect against an active attack on a communications system launched by an unauthorized party. According to Laurence et al., an active attack is one in which the unauthorized party injects a fraudulent simulation of a valid communication into the communication path. See col. 2, lns. 13-21. Where the communications system provides transactions for a financial network, for example, the unauthorized communications could result in the receiving station acting improperly,

such as by transferring funds to an account accessible to the unauthorized party. Accordingly, the object of Laurence et al. is to verify the authenticity of the sender of the data transmission--not to exchange keys between users. Unlike Laurence et al., the patent application is not directed to authentication, and there is no showing in the final Office Action that the authentication art is reasonably pertinent to the problem addressed by the applicants. See *In re Oetiker*, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). Indeed, the final Office Action includes no showing that persons skilled in the art would consider an authentication solution to be applicable to a problem of exchanging keys.

Even if the Board deems Laurence et al. pertinent to the invention, the final Office Action fails to present an adequate showing of motivation or suggestion to combine the references as required by the MPEP and other legal authority cited above. On this issue, the final Office Action merely concludes:

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key. One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent unauthorized access to the data.

See Office Action, page 5. This statement of motivation to combine the references cannot be found in either Menezes or Laurence et al. Menezes contains no statement, express or implied, indicating that it would be desirable to modify a data encrypting key using location identity data. Likewise, Laurence et al. contains no such teaching.

Responding to this specific issue raised by Appellant, the Advisory Action states: "the examiner draws the applicant's attention to Laurence's disclosure in col. 3 lines 65-67 who explicitly provides reasons for which modification of a data-encrypting key using location should be implemented." The quoted portion of the reference reads: "Each of the traditional active and passive attack prevention methods, no matter how complex, suffers from an inherent drawback: no protection is provided against an unauthorized party who has knowledge of the access code or the encryption key." Respectfully, this

statement shows merely the desirability of improved methods of authentication in preventing active and passive attacks. The statement shows no recognition of desirability of "modification of a data-encrypting key using location." Further, the statement shows no teaching or suggestion that conventional key exchange protocols be modified to include location information as an additional protection against unauthorized access to the data encrypting key. The assertion in the Advisory Action therefore falls woefully short of the required showing of motivation or suggestion to combine the references.

Moreover, there is no suggestion or motivation for the combination contained in the knowledge generally available to one of ordinary skill in the art. To the extent that the final Office Action relies upon such knowledge "generally available" in the art, it is the Examiner's burden of presenting evidence showing the state of such knowledge. *In re Lee*, 277 F.3d 1338, 1344-45, 61 USPQ2d 1430, 1434-35 (Fed. Circ. 2002). In this regard, the final Office Action does not include any such evidence and thereby fails to meet its burden.

Rather than reflecting the knowledge in the prior art, the stated motivation for the combination comes directly from the patent application itself. The patent application states:

This geo-encryption process comprises a method in which plaintext data is first encrypted using a random data encryption key that is generated at the time of encryption. The data encrypting key is then encrypted (or locked) using a location value and a key encrypting key. The encrypted data encrypting key is then transmitted to the receiver along with the ciphertext data. The receiver both must be at the correct location and must have a copy of a corresponding key decrypting key in order to derive the location key and decrypt the data encrypting key. After the data encrypting key is decrypted (or unlocked), it is used to decrypt the ciphertext. *If an attempt is made to decrypt the data encrypting key at an incorrect location or using an incorrect key decryption key, the decryption will fail.*

See page 4, line 22, through page 5, line 3. These statements plainly show that the motivation to "modify the data encrypting key using location identity data ... in order to

prevent unauthorized access to the data" originated with the patent application. The final Office Action therefore violates the Federal Circuit proscription against reliance on applicant's disclosure for a suggestion or motivation to combine prior art references. See *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

For at least this reason, the final Office Action fails to make a *prima facie* showing of obviousness with respect to the claims of Group I, mandating reversal of the rejection of these claims.

2. The proposed combination of Menezes and Laurence et al. fails to teach or suggest all the claim limitations

The final Office Action states that "Laurence et al. teach modifying (encryption) using a specific geographical location (Abstract and col. 23 lines 1-10) in order to prevent reading of the encrypted message by other receivers." Respectfully, this statement misses the point entirely and demonstrates the fundamental flaw of the final Office Action. As set forth in the claims of Group I, the invention is directed to the secure exchange of a data encrypting key by modifying it using location information, and not simply the encryption of messages. Appellant maintains that Laurence et al. contains no suggestion or disclosure of key exchange between sender and receiver, and specifically contains no suggestion or disclosure of the use of location information to modify a data encrypting key prior to communication to a receiver.

As discussed above, Laurence et al. is directed to the authentication of messages. To accomplish this object, Laurence et al. discloses the use of the position of the transmitter for authenticating each message that is received by a receiver. See col. 12, Ins. 49-54. "Since the transmitting location can be protected physically, it is very unlikely that an unauthorized user will be able to transmit from the proper transmitting location without detection." See col. 12, Ins. 58-62. The satellite system that carries the data transmissions can determine the location of the transmitter of each message that is received. See col. 13, Ins. 4-7. If proper authentication of the transmitter position does

not occur, the system can determine that an unauthorized message has been received. See col. 13, Ins. 9-12.

Laurence et al. discloses several embodiments of the message authentication system. In an exemplary embodiment shown in Fig. 4A, messages are encrypted using the transmitter position element, i.e., the actual location of the antenna of the transmitter. See col. 19, Ins. 27-36. As noted in the final Office Action, Laurence et al. further discloses that the position information of the intended receiver could also be used to encrypt the message. See col. 23, Ins. 1-3. The encrypted message is sent to the satellite, which then determines the location of the transmitter. See col. 19, Ins. 37-41. The transmitter location is then appended to the encrypted message and forwarded to the receiver at a second location. See col. 19, Ins. 41-44. The receiver then receives the encrypted message with the appended transmitter position data. See col. 19, Ins. 45-47. The receiver extracts the transmitter position data from the message and compares it against an authorized transmitter position stored in memory. See col. 19, Ins. 47-55. If the extracted position data matches the stored position data, the receiver determines that an authentic message was received and proceeds with decryption of the received message. See col. 19, Ins. 55-59.

Unlike the present invention, Laurence et al. does not use location data (either of the transmitter or the receiver) in a key exchange protocol. In fact, Laurence et al. contains no disclosure of key exchange whatsoever, and merely refers to the content of the data encrypting key as including location of the transmitter, the sender and/or non-position elements. See, e.g., col. 21, Ins. 21-30. In this regard, the Advisory Action erroneously states that Appellant "acknowledges that Laurence ... discloses a 'location-modified data encrypting key.'" Appellant disagrees with this characterization insofar as Laurence et al. discloses only the use of position information as a data element of the key, but fails to teach or suggest any use of position information to modify the key after its use in encrypting the digital information and prior to its encryption and subsequent communication to a receiver.

As discussed above, Menezes also fails to suggest or disclose this teaching, and discloses merely a "point-to-point key update" in which a random number selected as the session key is encrypted using a known encryption algorithm and key. Thus, even if combined as proposed, Menezes and Laurence et al. fail to suggest or disclose any use of location information to modify a data encrypting key or the encryption of a location-modified data encrypting key using a key encrypting key.

Accordingly, the proposed combination of references fails to suggest or disclose a method for controlling access to digital information comprising, *inter alia*, "modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key," as defined in the claims of Group I. It follows that the proposed combination of references further fail to suggest or disclose "encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key; and communicating said encrypted location-modified data encrypting key and said encrypted digital information to a recipient device such that said encrypted digital information can be decrypted by the recipient only at said specific geographic location," as also defined in the claims of Group I.

In view of the absence of any teaching or suggestion of these limitations in the proposed combination of references, the final Office Action fails to make a *prima facie* showing of obviousness with respect to the claims of Group I, mandating reversal of the rejection of these claims. Since all rejections in the final Office Action are based on the combination of Menezes and Laurence et al., resolution of the rejections of Group I in Appellant's favor will resolve all outstanding issues on appeal.

3. The other references of record fail to make up for the deficiencies of Menezes and Laurence et al.

The final Office Action includes rejections of the dependent claims of Group I based on further combinations of Menezes and Laurence et al. with other references,

including Murphy, Inoue et al., Jones et al. and Schneier. In view of the above showing that the combination of Menezes and Laurence et al. fails to suggest or disclose all limitations of independent Claims 1 and 28, these additional grounds of rejection are deemed moot. Moreover, these additional cited references fail to make up for the foregoing deficiencies of Menezes and Laurence et al., as will be further discussed below.

a. Murphy

The final Office Action acknowledges that the combination of Menezes and Laurence et al. fails to disclose that the "location identity data further comprise at least a location value and a proximity value of the specific geographic location of the recipient and that a GPS receiver is used in recovering the location."

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location stored in the receiver/processor for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated.

Murphy does not use location data in the encryption of keys used to protect the underlying digital information, and therefore has no applicability to the present patent application. Instead, Murphy is directed to a one-to-many communication system in which the same encrypted signals are sent to many users. There is nothing distinctive about the encrypted signals that reflects a transformation using data defining a specific

geographic location. In fact, the encrypted signals themselves have no relation to the location information whatsoever. Instead, Murphy uses location information only to determine whether to activate the decryption chip. The SATPS location signal is compared to location information that is previously stored in the receiver, and which has nothing to do with the encrypted signals. Notably, this determination occurs whenever the set-top box (i.e., receiver) is turned on or after the power supply is interrupted (see col. 8, lines 6-24 and 46-62), i.e., without any consideration of the encrypted signals.

b. Inoue et al.

The final Office Action acknowledges that the combination of Menezes and Laurence et al. "do not teach decrypting and re-encrypting a location modified data encrypting key." To make up for this deficiency, the final Office Action proposes the further combination with Inoue et al.

Inoue et al. discloses a packet processing system that eliminates redundant encryption/decryption of message packets passing through intermediate agents between sender and recipient. According to the reference, when relaying encrypted packets of digital information, each node in the relay will decrypt and then re-encrypt the packet. Notably, the Inoue et al. packet processing system does not use location data to encrypt the packet encrypting key. In this respect, Inoue et al. suffers from the same deficiency as Menezes and the other references.

c. Jones et al.

The final Office Action acknowledges that the combination of Menezes and Laurence et al. "do not teach decrypting and re-encrypting location-modified data encrypting key." To make up for this deficiency, the final Office Action proposes the further combination with Jones et al.

Jones et al. disclose an encryption chip that is programmable to process a variety of secret key and public key encryption algorithms. The reference discloses a

link encryption application in which encrypted data received at a router between successive links is first decrypted by the chip and then the data is re-encrypted in accordance with the encryption algorithm of the next link. See col. 5, Ins. 49-55. Jones et al. fails to suggest or disclose any use of location information as any part of the link encryption. More specifically, Jones et al. fails to suggest or disclose any modifying of a data encrypting key or encrypting of a location-modified data encrypting key using a key encrypting key, and therefore fails to make up for the deficiencies of Menezes and Laurence et al. discussed above.

d. Schneier

The final Office Action acknowledges that “none of the references explicitly teach that generating the encryption key comprises using GPS signals to partially seed the pseudo-random number generator.” To make up for this deficiency, the final Office Action proposes the further combination with Schneier.

Schneier provides a general text showing the current state of cryptography. The final Office Action states that “Schneier teach generating the data encrypting key using a pseudo-random number generator.” Even if true, there is no teaching or suggestion in the reference of using GPS signals to partially seed the pseudo-random number generator. Schneier otherwise fails to suggest or disclose any modifying of a data encrypting key or encrypting of a location-modified data encrypting key using a key encrypting key, and therefore fails to make up for the deficiencies of Menezes and Laurence et al. discussed above.

B. Group II (Claims 45-48)

Independent Claim 45 of Group II is directed to an apparatus for receiving digital information having a processor operable to perform the following functions:

receiving encrypted digital information and an encrypted location-modified data encrypting key;

decrypting said encrypted location-modified data encrypting key using a key encrypting key to obtain a location-modified data encrypting key;

determining a location value that defines a specific geographic location of said apparatus;

extracting a data encrypting key from said location-modified data encrypting key using said location value; and

decrypting said encrypted digital information using said data encrypting key.

Hence, the claims of Group II are directed primarily to the receipt and decryption of digital information and the data encrypting key using location information defining a specific geographic location of the receiver. In other words, the claims of Group II cover the receiver side of the communication interface.

For the same reasons presented with respect to Group I, there is no teaching or suggestion for the proposed combination of Menezes and Laurence et al. Furthermore, the proposed combination of Menezes and Laurence et al. fails to suggest or disclose all limitations of the claims of Group II. As discussed above, the Laurence et al. receiver receives an encrypted message with appended position data (for either the transmitter or receiver). See col. 19, Ins. 45-47. The receiver extracts the position data from the message and compares it against an authorized position stored in memory. See col. 19, Ins. 47-55. If the extracted position data matches the stored position data, the receiver determines that an authentic message was received and proceeds with decryption of the received message using the position data as a decryption key. See col. 19, Ins. 55-59. Hence, Laurence et al. uses the position data only to authenticate the message and not to provide a layer of security on top of the data encrypting key. The Laurence et al. receiver does not receive a "location-modified data encrypting key" and does not extract a data encrypting key from a location-modified data encrypting key using location data.

Accordingly, the proposed combination of references fails to suggest or disclose an apparatus for receiving digital information comprising a processor providing the

functions of, *inter alia*, "decrypting said encrypted location-modified data encrypting key using a key encrypting key to obtain a location-modified data encrypting key; ... [and] extracting a data encrypting key from said location-modified data encrypting key using said location value," as defined in the claims of Group II. In view of the absence of any teaching or suggestion of these limitations in the proposed combination of references, the final Office Action fails to make a *prima facie* showing of obviousness with respect to the claims of Group II, mandating reversal of the rejection of these claims.

Murphy, Inoue et al., Jones et al. and Schneier fail to make up for the deficiencies of Menezes and Laurence et al. None of these secondary references suggest or disclose any use of a "location-modified data encrypting key" or the extraction of a data encrypting key from a location-modified data encrypting key using location data.

C. Group III (Claims 21-27, 41-44 and 49-50)

The claims of Group III are directed to the methods and apparatus discussed above with addition of a "key table used to store a plurality of keys including said key encrypting key" (i.e., Claims 21, 41, and 49). These claims further add limitations relating to administering management of the plurality of keys (i.e., Claims 23-26, 41), storing keys used for signing data and/or validating signatures (i.e., Claims 27, 44), and associating keys with respective providers of digital information (i.e., Claims 22, 42, 50).

The final Office Action acknowledges that Menezes and Laurence et al. "do not explicitly teach a key table used for storing a plurality of keys including a key encrypting key." See Office Action, page 9. To make up for this deficiency, the final Office Action proposes the further combination with Shibata et al.

Shibata et al. discloses a system for communicating encrypted information, and includes a cipher key table in which a plurality of cipher keys are stored. More specifically, Shibata et al. discloses a facsimile machine having a space in random access memory in which is stored the cipher key table. See col. 7, Ins. 20-22. The

cipher keys are selectively used to encrypt outgoing facsimile messages. See col. 8, Ins. 60-64. The user of the facsimile machine can enter a number as a cipher key using function keys in a keypad. See col. 15, ln. 61 through col. 16, ln. 17. The user can also alter and delete cipher keys using the same function keys. See col. 16, Ins. 18-37.

As a threshold matter, Shibata et al. contains no suggestion or disclosure of a location-modified data encrypting key or the modification or extraction of a data encrypting key using location data. Hence, as an initial matter, the reference fails to make up for the deficiencies of Menezes and Laurence et al. discussed above. Appellant therefore maintains that the claims of Group III are allowable in view of the above showing that the independent claims of Groups I and II are allowable.

Even if Menezes and Laurence et al. were construed as suggesting or disclosing the independent claims, there is no teaching or suggestion for the further combination with Shibata et al. and the reference fails to suggest or disclose the further limitations of Group III. Similar to Laurence et al., Shibata et al. does not address key exchange between a sender and receiver. Instead, Shibata et al. discloses only the administration of a cipher key table by the operator of the facsimile machine. There is no disclosure in Shibata et al. of any remote administration of the cipher key table, nor is there any disclosure of an ability to receive cipher keys remotely from a sender of digital information. For these reasons, the key table of Shibata et al. would be unsuitable in a system and method for communicating an encrypted, location-modified data encrypting key between a sender and receiver. Indeed, the final Office Action identifies no teaching or suggestion for the proposed combination of references.

Accordingly, the final Office Action fails to make a *prima facie* showing of obviousness with respect to the claims of Group III, mandating reversal of the rejection of these claims.

The final Office Action also rejects the claims of Group III over the combination of Menezes and Laurence et al. as discussed above and further in view of Schneier. Appellant deems this ground of rejection erroneous insofar as the final Office Action

identifies no teaching or suggestion of Schneier pertinent to the use of a key table for storing a plurality of keys including a key encrypting key. Instead, the final Office Action refers only to the reference's teaching of generating a data encrypting key using a pseudo-random number generator, which is a feature that is not recited in any of the claims of Group III. Appellant noted this defect of the final Office Action in Appellant's response submitted on February 27, 2006, but the Advisory Action failed to withdraw or clarify the ground of rejection. The Board should reverse this ground of rejection as unsupported by the record.

D. Group IV (Claims 16-17 and 38)

The claims of Group IV are directed to the methods and apparatus discussed above with addition of "routing said encrypted digital information to an intended receiver through at least one distributor" (i.e., Claims 16 and 38) and "adding a layer of encryption of said data encrypting key for said at least one distributor" (i.e., Claim 17).

The final Office Action fails to identify any particular teaching of the references showing these features. Instead, the final Office Action relies upon Official Notice:

As per claims 16 and 38 Official Notice is taken that it is old and well-known practice to engage at least one distributor (intermediate node) when routing (encrypted and non-encrypted) digital information. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ at least one distributor in order to be able to route information to various remote recipients.

See Office Action, pages 5-6. This statement of Official Notice is a gross oversimplification of the invention to the extent that the claims do not merely recite routing of information through a distributor. To the contrary, the claims recite communicating an encrypted, location-modified data encrypting key between a sender and receiver and through at least one distributor. The final Office Action identifies no teaching or suggestion for use of a distributor within a method or system for communicating an encrypted, location-modified data encrypting key as set forth in the claims.

Moreover, the final Office Action's reliance upon Official Notice contravenes the

guidance set forth in MPEP § 2144.03. Official notice unsupported by documentary evidence should only be taken where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known. See MPEP § 2144.03(A). Any facts so noticed should be of notorious character and serve only to “fill in the gaps” in an insubstantial manner which might exist in the evidentiary showing made to support a particular ground for rejection. See MPEP § 2144.03(E).

In this case, the noticed facts are not merely filling gaps in the reference but rather constitute the principle evidence upon which the rejection was based. This is an inappropriate basis for rejection of the claims. See MPEP § 2144.03(A) (“It is never appropriate to rely solely on ‘common knowledge’ in the art without evidentiary support in the record, as the principle evidence upon which a rejection was based.”); see also *In re Zurko*, 258 F.3d 1379, 1385, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001) (“[T]he Board cannot simply reach conclusions based on its own understanding or experience--or on its assessment of what would be basic knowledge or common sense. Rather, the Board must point to some concrete evidence in the record in support of these findings.”)

The final Office Action also relies upon further combinations of Menezes and Laurence et al. with Inoue et al. and Jones et al. as showing data that has been successively encrypted and re-encrypted along a path between sender and receiver. See Office Action, pages 11-12. As discussed above with respect to the claims of Group I, neither Inoue et al. or Jones et al. suggest or disclose any modifying of a data encrypting key or encrypting of a location-modified data encrypting key using a key encrypting key, and therefore fails to make up for the deficiencies of Menezes and Laurence et al. discussed above. The final Office Action therefore fails to make a *prima facie* showing of obviousness with respect to the claims of Group IV, mandating reversal of the rejection of these claims.

Serial No. 09/992,378
May 1, 2006
Page 25

Conclusion

For the foregoing reasons, applicants and Appellant respectfully submit that the rejections of Claims 1-6, 8-32, and 34-50 were improper and should be reversed.

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'B. Berliner', written over a horizontal line.

Brian M. Berliner
Attorney for Appellant
Registration No. 34,549

Date: May 1, 2006

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000

APPENDIX A
LISTING OF CLAIMS

1. (Previously presented) A method for controlling access to digital information, comprising:

encrypting said digital information using a data encrypting key;
modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key;
encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key; and
communicating said encrypted location-modified data encrypting key and said encrypted digital information to a recipient device such that said encrypted digital information can be decrypted by the recipient only at said specific geographic location.

2. (Previously presented) The method of Claim 1, wherein said location identity data further comprises at least a location value and a proximity value of said specific geographic location.

3. (Previously presented) The method of Claim 2, wherein said location value defines a location of an intended receiver of said digital information.

4. (Original) The method of Claim 2, wherein said location value further comprises at least one of a latitude, longitude, altitude and time dimension.

5. (Previously presented) The method of Claim 2, wherein said location identity data further defines a universal location that encompasses the entire earth.

6. (Previously presented) The method of Claim 3, wherein said proximity value defines a zone that encompasses said location.

7. (Cancelled)

8. (Original) The method of Claim 1, further comprising identifying location of a receiver at which access to said digital information is sought.

9. (Original) The method of Claim 8, wherein said location identifying step further comprises recovering said location from a GPS receiver.

10. (Previously presented) The method of Claim 1, wherein said location identity data further comprises a location value and a shape parameter, the shape parameter defining a shape of a region encompassing the specific geographic location.

11. (Previously presented) The method of Claim 1, further comprising:
 decrypting said encrypted location-modified data encrypting key
 using a key decrypting key;
 using a location value to recover said data encrypting key from said
 location-modified data encrypting key; and
 decrypting said digital information using said data encrypting key.

12. (Previously presented) The method of Claim 11, further comprising deriving said location value from a signal received by a GPS receiver and a shape parameter defining a shape of a region encompassing the specific geographic location.

13. (Original) The method of Claim 1, wherein said digital information further comprises a secret key, and further comprising the step of distributing said secret key to an intended receiver.

14. (Previously presented) The method of Claim 11, further comprising precluding ability to decrypt said encrypted digital information if said step of decrypting said encrypted digital information is attempted at other than said specific geographic location.

15. (Previously presented) The method of Claim 11, further comprising precluding ability to decrypt said encrypted digital information if said step of decrypting said encrypted digital information is attempted without using said key decrypting key.

16. (Original) The method of Claim 1, further comprising routing said encrypted digital information to an intended receiver through at least one distributor.

17. (Original) The method of Claim 16, wherein said routing step further comprises adding a layer of encryption of said data encrypting key for said at least one distributor.

18. (Previously presented) The method of Claim 1, further comprising generating said data encrypting key using a pseudo-random number generator.

19. (Previously presented) The method of Claim 18, wherein said step of generating said data encrypting key further comprises using GPS signals to partially seed said pseudo-random number generator.

20. (Previously presented) The method of Claim 1, further comprising decrypting and recovering said data encrypting key from said encrypted location-modified data encrypting key using a key decrypting key and a location value, and re-encrypting said data encrypting key using at least one of a different location identity data and a different key encrypting key to produce a different encrypted location-modified data encrypting key.

21. (Original) The method of Claim 1, further comprising providing a key table used to store a plurality of keys including said key encrypting key.

22. (Original) The method of Claim 21, further comprising associating said plurality of keys with respective providers of said digital information.

23. (Original) The method of Claim 21, further comprising administering management of said plurality of keys in said key table.

24. (Original) The method of Claim 23, wherein said administering step further comprises adding, changing or deleting any one of said plurality of keys in said key table.

25. (Original) The method of Claim 23, wherein said key table is located with a remote device, and said administering step further comprises adding, changing or deleting any one of said plurality of keys in said key table remotely.

26. (Original) The method of Claim 25, wherein said administering step further comprises including a signature when adding, changing or deleting any one of said plurality of secret keys in said key table.

27. (Original) The method of Claim 21, wherein said step of providing a key table further comprises storing keys used for signing data and validating signatures.

28. (Previously presented) An apparatus for controlling access to digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

encrypting said digital information using a data encrypting key;

modifying the data encrypting key using location identity data that defines at least a specific geographic location to produce a location-modified data encrypting key;

encrypting said location-modified data encrypting key using a key encrypting key to produce an encrypted location-modified data encrypting key; and

communicating said encrypted location-modified data encrypting key and said encrypted digital information to a recipient device such that said encrypted digital information can be decrypted by the recipient only at said specific geographic location.

29. (Previously presented) The apparatus of Claim 28, wherein said location identity data comprises at least a location value and a proximity value of said specific geographic location.

30. (Previously presented) The apparatus of Claim 29, wherein said location value defines a location of an intended receiver of said digital information.

31. (Original) The apparatus of Claim 29, wherein said location value further comprises at least one of a latitude, longitude, altitude and time dimension.

32. (Original) The apparatus of Claim 29, wherein said proximity value corresponds to a zone that encompasses said location.

33. (Cancelled)

34. (Original) The apparatus of Claim 28, wherein said processor is further operable to identify location of a receiver at which access to said digital information is sought.

35. (Original) The apparatus of Claim 28, further comprising a GPS receiver coupled to said processor.

36. (Previously presented) The apparatus of Claim 28, wherein said location identity data further comprises a location value and a shape parameter, the shape parameter defining a shape of a region encompassing said specific geographic location.

37. (Original) The apparatus of Claim 28, wherein said digital information further comprises a secret key, and said processor is further operable to distribute said secret key to an intended receiver located at said specific geographic location.

38. (Original) The apparatus of Claim 28, wherein said processor is further operable to route said encrypted digital information to an intended receiver through at least one distributor.

39. (Original) The apparatus of Claim 28, further comprising a pseudo-random number generator operatively coupled to said processor to generate said data encrypting key.

40. (Previously presented) The apparatus of Claim 28, wherein said processor is further operable to decrypt said encrypted location-modified data encrypting key, and re-encrypt said location-modified data encrypting key using at least one of a different location identity data and a different key encrypting key.

41. (Original) The apparatus of Claim 28, wherein said memory further comprises a key table used to store a plurality of keys including said key encrypting key.

42. (Original) The apparatus of Claim 41, wherein ones of said plurality of keys are associated with respective providers of said digital information.

43. (Original) The apparatus of Claim 41, wherein processor is further operable to add, change or delete any one of said plurality of keys in said key table.

44. (Original) The method of Claim 41, wherein said processor is further operable to provide a signature for authentication of one of said plurality of keys.

45. (Previously presented) An apparatus for receiving digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

receiving encrypted digital information and an encrypted location-modified data encrypting key;

decrypting said encrypted location-modified data encrypting key using a key encrypting key to obtain a location-modified data encrypting key;

determining a location value that defines a specific geographic location of said apparatus;

extracting a data encrypting key from said location-modified data encrypting key using said location value; and

decrypting said encrypted digital information using said data encrypting key.

46. (Previously presented) The apparatus of Claim 45, wherein said function of decrypting said encrypted digital information further comprises precluding ability to decrypt said encrypted digital information if decryption is attempted at other than said specific geographic location.

47. (Original) The apparatus of Claim 45, further comprising a GPS receiver coupled to said processor.

48. (Previously presented) The apparatus of Claim 45, wherein said processor is further operable to re-encrypt said data encrypting key using at least one of a different location identity data and a different key encrypting key.

49. (Original) The apparatus of Claim 45, wherein said memory further comprises a key table used to store a plurality of keys including said key decrypting key.

50. (Original) The apparatus of Claim 45, wherein ones of said plurality of keys are associated with respective providers of said digital information.

Serial No. 09/992,378
May 1, 2006
Page 34

APPENDIX B
EVIDENCE RELIED UPON BY APPELLANT

None

Serial No. 09/992,378
May 1, 2006
Page 35

APPENDIX C
RELATED PROCEEDINGS

None